ESET Research discovers Operation Jacana, targeting governmental entity in Guyana, likely by Chinese threat group

DUBAI , DUBAI, UNITED ARAB EMIRATES, October 9, 2023 /EINPresswire.com/ -- ESET researchers discovered a cyberespionage campaign against a governmental entity in Guyana. Named Operation Jacana by ESET, we believe with medium confidence that it is linked to a China-aligned threat group. In the attack, the operators used a previously undocumented backdoor, DinodasRAT (Remote Access Trojan), that can exfiltrate files, manipulate Windows registry keys, and execute commands, and it encrypts the information it sends to the command and control server (C&C) using the Tiny Encryption Algorithm.

This campaign was targeted, as the threat actors crafted their emails specifically to entice their chosen victim organization. After successfully compromising an initial but limited set of machines with DinodasRAT, the operators proceeded to move inside and breach the target's internal network, where they again deployed this backdoor. It has various capabilities that allow an attacker to spy on and collect sensitive information from a victim's computer. Other malicious tools, such as a variant of Korplug (aka PlugX), were also deployed.

Korplug is common to China-aligned groups, for example, Mustang Panda. The attribution to a China-aligned threat actor is made with only medium confidence. This attribution is further supported by recent developments in Guyana–China diplomatic relations. In February 2023, the same month that Operation Jacana took place, the Special Organized Crime Unit of Guyana arrested three people in a money-laundering investigation involving Chinese companies, an act disputed by the local Chinese embassy.

The deployed spearphishing emails referenced recent Guyanese public and political affairs, indicating that the attackers are keeping track of their victims' (geo)political activities to increase the likelihood of the operation's success. One email, luring the victims with news concerning a

“Guyanese fugitive in Vietnam,” contained a domain ending with gov.vn. “This domain indicates a Vietnamese governmental website; thus, we believe that the operators were able to compromise a Vietnamese governmental entity and use its infrastructure to host malware samples. ESET researchers notified the VNCERT about the compromised infrastructure,” says ESET researcher Fernando Tavella, who discovered Operation Jacana.

ESET researchers have named the backdoor DinodasRAT based on the victim identifier it sends to its C&C server: the string always begins with Din, which reminded us of the hobbit Dinodas from the Lord of the Rings by J.R.R. Tolkien. On the other hand, wattled jacanas are birds native to Guyana; they sport large claws on their feet, allowing them to walk on floating plants in the lakes they inhabit.

For more technical information about Operation Jacana and the DinodasRAT backdoor, check out the blog post “Operation Jacana: Foundling hobbits in Guyana” on WeLiveSecurity. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET’s high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET’s R&D centers worldwide, working in support of our shared future. For more information,
visit www.eset.com or follow us on LinkedIn, Facebook and Twitter.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here